Claims

1. A method for effecting payments comprising steps of: replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator; performing an operation of opening a payee's account; performing a payment operation in which the payment certificate signature and an identifier of the payment certificate base are included into payment data delivered to a payee device by means of which a payee order is formed including the payment certificate signature and the identifier of the payment certificate base; delivering the formed payee order to a payment server in which the payee's account is credited on the basis of the payee order in the case of absence of an information that the payment certificate was utilized, according to the validity of the delivered payment certificate signature; and forming the operator's response to the payee order, by means of which response the payment operation is judged, *characterized* in that the method is further comprising steps of: including an identifier of a public key into the payment certificate base, said public key corresponding to an arbitrary secret key of a payer, wherein the public key is accepted as a public key of the payment certificate and the secret key of the payer is accepted as a secret key of the payment certificate; including a payer order signed with the secret key of the payment certificate into the payment data, and including an information on the payee and the identifier of the payment certificate base into the payer order; and the step of crediting the payee's account is carried out according to the validity of the signature on the payer order.

2. The method according to claim 1, *characterized* in that in the step of performing the payment operation the signed payer order is entered into the operator's information storage.

3. The method according to claim 1, *characterized* in that in the step of replenishing the payer device a money demand is formed including data for making a blind money signature, and is delivered to the payment server in which a replenishment source and replenishment amount are determined according to the money demand; data to be unblinded are created in the step of making the blind money signature by processing data for making the blind money signature, that are comprised in the demand, with a secret money key corresponding to the replenishment amount, whereupon the payment certificate signature is made in the payer device by unblinding.

4. The method according to claim 3, *characterized* in that in the step of replenishing the payer device by the operation of primarily filling the payment certificate a blinded identifier of the created payment certificate base is included as the data for making the blind money signature into the money demand being formed.

5. The method according to claim 1, *characterized* in that in the step of performing the payment operation a payee receipt is included into the operator's response to the payee order, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payee is judged according to the validity of the signature on the payee receipt.

6. The method according to claim 1, *characterized* in that in the step of performing the payment operation data are formed in the payee device with the use of the operator's response to the payee order and delivered to the payer device, according to which data the

performing of the payment for the payer is judged.

7. The method according to claim 6, *characterized* in that in the step of performing the payment operation a payer receipt is included into the operator's response to the payee order and into the data delivered to the payer device, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payer is judged according to the validity of the signature on the payer receipt.

8. The method according to claim 7, *characterized* in that the payer receipt is encrypted by an arbitrary encryption key of the payer prior to including said receipt into the operator's response to the payee order.

9. The method according to claim 1, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate converted by an arbitrary one-way function is used as the identifier of the payment certificate base.

10. The method according to claim 1, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate.

11. The method according to claim 1, *characterized* in that in the step of replenishing the payer device the validity of the made payment certificate signature is verified.

12. The method according to claim 1, *characterized* in that in the step of opening the account an arbitrary secret key is accepted as the secret key of the account, and the public key corresponding to the secret key of the account is delivered to the payment server as a public key of the account being opened.

13. The method according to claim 1, *characterized* in that conditions of payment are included into the payer order.

14. The method according to claim 13, *characterized* in that payee obligation data are included into the conditions of payment comprised in the payer order.

15. The method according to claim 14, *characterized* in that prior to performing the payment operation, the payee obligation data are signed with an arbitrary secret key of the payee, and the payer verifies the payee's signature on the payee obligation data prior to performing the payment operation.

16. The method according to claim 13, *characterized* in that in the payer device in the step of forming the payment data, the payee obligation data are processed by an arbitrary one-way function, and data obtained in this processing are included into the payer order as the conditions of payment.

17. The method according to claim 1, *characterized* in that the payer order is encrypted by an arbitrary public encryption key of the operator prior to including them into the payment data.

18. The method according to claim 1, *characterized* in that in the step of replenishing the payer device a payer's account is used as a replenishment source.

19. The method according to claim 1, *characterized* in that in the step of replenishing the payer device a bank card is used as a replenishment source.

20. The method according to claim 1, *characterized* in that in the step of performing the payment operation the payee appears as the payer.

21. The method according to claim 1, *characterized* in that in the step of performing the payment operation a part of a payment certificate value is returned to the payer device.

22. The method according to claim 1, *characterized* in that the step of replenishing the payer device is performed from funds of an intermediate payer.

23. The method according to claim 22, *characterized* in that in the step of replenishing the payer device, data blinded in the payer device in the step of making the blind money signature of the operator are subjected to an additional blinding in the payer device of the intermediate payer.

24. A method for effecting payments comprising steps of: replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator; performing an operation of opening a payee's account; performing a payment operation in which the payment certificate signature and an identifier of the payment certificate base are included into payment data delivered to a payee device by means of which a payee order is formed including the payment certificate signature and the identifier of the payment certificate base; delivering the formed payee order to a payment server in which the payee's account is credited on the basis of the payee order in the case of absence of an information that the payment certificate was utilized, according to the validity of the delivered payment certificate signature; and forming the operator's response to the payee order, by means of which response the payment operation is judged, *characterized* in that the method is further comprising steps of: including an identifier of a public key into the payment certificate base, said public key corresponding to an arbitrary secret key of the payee, wherein the public key is accepted as a public key of the payment certificate and the secret key of the payee is accepted as a secret key of the payment certificate; performing the replenishment of the payer device by means of an operation of replenishing the payment certificate, in which operation a blind money signature of the operator on the payment certificate signature already being in the payer device is made; including a payer order signed with the secret key of the payment certificate into the payment data, and including an information on the payee and the identifier of the payment certificate base into the payer order; and the step of crediting the payee's account is carried out according to the validity of the signature on the payer order.

25. The method according to claim 24, *characterized* in that in the step of replenishing the payer device a money demand is formed including data for making a blind money signature, and is delivered to the payment server in which a replenishment source and replenishment amount are determined according to the money demand; data to be unblinded are created in the step of making the blind money signature by processing data for making the blind money signature, that are comprised in the demand, with a secret money key corresponding to the replenishment amount, whereupon the payment certificate signature is made in the payer device by unblinding.

26. The method according to claim 25, *characterized* in that in the step of replenishing the payer device by the operation of primarily filling the payment certificate a blinded identifier of the created payment certificate base is included as the data for making the blind money signature into the money demand being formed.

27. The method according to claim 25, *characterized* in that in the step of replenishing the payer device by the operation of replenishing the payment certificate a blinded payment certificate signature is included as the data for making the blind money signature into the money demand being formed.

28. The method according to claim 24, *characterized* in that in the step of performing the payment operation the signed payer order is entered into the operator's information storage.

29. The method according to claim 24, *characterized* in that in the step of performing the payment operation a payee receipt is included into the operator's response to the payee order, which receipt being signed with the arbitrary secret key of the operator, and the per-

forming of the payment for the payee is judged according to the validity of the signature on the payee receipt.

30. The method according to claim 24, *characterized* in that in the step of performing the payment operation data are formed in the payee device with the use of the operator's response to the payee order and delivered to the payer device, according to which data the performing of the payment for the payer is judged.

31. The method according to claim 30, *characterized* in that in the step of performing the payment operation a payer receipt is included into the operator's response to the payee order and into the data delivered to the payer device, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payer is judged according to the validity of the signature on the payer receipt.

32.. The method according to claim 31, *characterized* in that the payer receipt is encrypted by an arbitrary encryption key of the payer prior to including said receipt into the operator's response to the payee order.

33. The method according to claim 24, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate converted by an arbitrary one-way function is used as the identifier of the payment certificate base.

34. The method according to claim 24, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate.

35. The method according to claim 24, *characterized* in that in the step of replenishing the payer device the validity of the made payment certificate signature is verified.

36. The method according to claim 24, *characterized* in that in the step of opening the account an arbitrary secret key is accepted as the secret key of the account, and the public key corresponding to the secret key of the account is delivered to the payment server as a public key of the account being opened.

37. The method according to claim 24, *characterized* in that conditions of payment are included into the payer order.

38. The method according to claim 37, *characterized* in that payee obligation data are included into the conditions of payment comprised in the payer order.

39. The method according to claim 38, *characterized* in that prior to performing the payment operation, the payee obligation data are signed with an arbitrary secret key of the payee, and the payer verifies the payee's signature on the payee obligation data prior to performing the payment operation.

40. The method according to claim 38, *characterized* in that in the payer device in the step of forming the payment data, the payee obligation data are processed by an arbitrary one-way function, and data obtained in this processing are included into the payer order as the conditions of payment.

41. The method according to claim 24, *characterized* in that the payer order is encrypted by an arbitrary public encryption key of the operator prior to including them into the payment data.

42. The method according to claim 24, *characterized* in that in the step of replenishing the payer device a payer's account is used as a replenishment source.

43. The method according to claim 24, *characterized* in that in the step of replenishing the

payer device a bank card is used as a replenishment source.

44. The method according to claim 24, *characterized* in that in the step of performing the payment operation the payee appears as the payer.

45. The method according to claim 24, *characterized* in that in the step of performing the payment operation a part of a payment certificate value is returned to the payer device.

46. The method according to claim 24, *characterized* in that the step of replenishing the payer device is performed from funds of an intermediate payer.

47. The method according to claim 46, *characterized* in that in the step of replenishing the payer device, data blinded in the payer device in the step of making the blind money signature of the operator are subjected to an additional blinding in the payer device of the intermediate payer.

48. A method for effecting payments comprising steps of: replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator; performing an operation of opening a payee's account; performing a payment operation in which an identifier of the payment certificate base is included into payment data delivered to a payee device by means of which a payee order is formed including the identifier of the payment certificate base received from a payer; delivering the formed payee order to a payment server in which the payee's account is credited on the basis of the payee order; forming the operator's response to the payee order, by means of which response the payment operation is judged, *characterized* in that the method is further comprising steps of: including an identifier of a public key into the payment certificate base, said public key corresponding to an arbitrary secret key of a payer, wherein the public key is accepted as a public key of the payment certificate and the secret key of the payer is accepted as a secret key of the payment certificate; opening a payment account associated with the payment certificate base; carrying out the operation of crediting the payment account, in which a payment certificate signature is delivered to the payment server, choosing the level of said signature arbitrarily within the level of the payment certificate, and the operation of crediting the payment account is carried out in accordance with the excess of the level of the delivered signature above the level of the payment account; including a payer order signed with the secret key of the payment certificate into the payment data, and including an information on the payee and the identifier of the payment certificate base into the payer order; and the step of crediting the payee's account is carried out according to the validity of the signature on the payer order from funds of the payment account.

49. The method according to claim 48, *characterized* in that the payment account associated with the payment certificate base is opened in the step of performing the payment operation.

50. The method according to claim 48, *characterized* in that the crediting operation is carried out in the step of performing the payment operation.

51. The method according to claim 48, *characterized* in that in the step of performing the payment operation the signed payer order is entered into the operator's information storage.

52. The method according to claim 48, *characterized* in that in the step of replenishing the payer device a money demand is formed including data for making a blind money signature, and is delivered to the payment server in which a replenishment source and replenishment amount are determined according to the money demand; data to be unblinded are created in the step of making the blind money signature by processing data for making the blind money signature, that are comprised in the demand, with a secret money key corresponding to the replenishment amount, whereupon the payment certificate signature is made in the payer device by unblinding.

53. The method according to claim 52, *characterized* in that in the step of replenishing the payer device by the operation of primarily filling the payment certificate a blinded identifier of the created payment certificate base is included as the data for making the blind money signature into the money demand being formed.

54. The method according to claim 48, *characterized* in that in the step of performing the

payment operation a payee receipt is included into the operator's response to the payee order, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payee is judged according to the validity of the signature on the payee receipt.

55. The method according to claim 48, *characterized* in that in the step of performing the payment operation data are formed in the payee device with the use of the operator's response to the payee order and delivered to the payer device, according to which data the performing of the payment for the payer is judged.

56. The method according to claim 55, *characterized* in that in the step of performing the payment operation a payer receipt is included into the operator's response to the payee order and into the data delivered to the payer device, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payer is judged according to the validity of the signature on the payer receipt.

57. The method according to claim 56, *characterized* in that the payer receipt is encrypted by an arbitrary encryption key of the payer prior to including said receipt into the operator's response to the payee order.

58. The method according to claim 48, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate converted by an arbitrary one-way function is used as the identifier of the payment certificate base.

59. The method according to claim 48, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate.

60. The method according to claim 48, *characterized* in that in the step of replenishing the payer device the validity of the made payment certificate signature is verified.

61. The method according to claim 48, *characterized* in that in the step of opening the account an arbitrary secret key is accepted as the secret key of the account, and the public key corresponding to the secret key of the account is delivered to the payment server as a public key of the account being opened.

62. The method according to claim 48, *characterized* in that conditions of payment are included into the payer order.

63. The method according to claim 62, *characterized* in that payee obligation data are included into the conditions of payment comprised in the payer order.

64. The method according to claim 63, *characterized* in that prior to performing the payment operation, the payee obligation data are signed with an arbitrary secret key of the payee, and the payer verifies the payee's signature on the payee obligation data prior to performing the payment operation.

65. The method according to claim 62, *characterized* in that in the payer device in the step of forming the payment data, the payee obligation data are processed by an arbitrary one-way function, and data obtained in this processing are included into the payer order as the conditions of payment.

66. The method according to claim 48, *characterized* in that the payer order is encrypted by an arbitrary public encryption key of the operator prior to including them into the payment data.

67. The method according to claim 48, *characterized* in that in the step of replenishing the

payer device a payer's account is used as a replenishment source.

68. The method according to claim 48, *characterized* in that in the step of replenishing the payer device a bank card is used as a replenishment source.

69. The method according to claim 48, *characterized* in that in the step of performing the payment operation the payee appears as the payer.

70. The method according to claim 48, *characterized* in that in the step of performing the payment operation a part of a payment certificate value is returned to the payer device.

71. The method according to claim 48, *characterized* in that in the step of replenishing the payer device, a payment account associated with the base of one of payment certificates is used as a replenishment source.

72. The method according to claim 48, *characterized* in that the step of replenishing the payer device is performed from funds of an intermediate payer.

73. The method according to claim 72, *characterized* in that in the step of replenishing the payer device, data blinded in the payer device in the step of making the blind money signature of the operator are subjected to an additional blinding in the payer device of the intermediate payer.

74. A method for effecting payments comprising steps of: replenishing a payer device by an operation of primarily filling a payment certificate, in which a payment certificate base is created in the payer device and a payment certificate signature is obtained by means of making a blind money signature of an operator; performing an operation of opening a payee's account; performing a payment operation in which an identifier of the payment certificate base is included into payment data delivered to a payee device by means of which a payee order is formed including the identifier of the payment certificate base received from a payer; delivering the formed payee order to a payment server in which the payee's account is credited on the basis of the payee order; forming the operator's response to the payee order, by means of which response the payment operation is judged, *characterized* in that the method is further comprising steps of: including an identifier of a public key into the payment certificate base, said public key corresponding to an arbitrary secret key of a payer, wherein the public key is accepted as a public key of the payment certificate and the secret key of the payer is accepted as a secret key of the payment certificate; performing the operation of replenishing the payer device by an operation of replenishing the payment certificate, in which a blind money signature of the operator on the payment certificate signature already being in the payer device is made; opening a payment account associated with the payment certificate base; carrying out the operation of crediting the payment account, in which a payment certificate signature is delivered to the payment server, choosing the level of said signature arbitrarily within the level of the payment certificate, and the operation of crediting the payment account is carried out in accordance with the excess of the level of the delivered signature above the level of the payment account; including a payer order signed with the secret key of the payment certificate into the payment data, and including an information on the payee and the identifier of the payment certificate base into the payer order; and the step of crediting the payee's account is carried out according to the validity of the signature on the payer order from funds of the payment account.

75. The method according to claim 74, *characterized* in that the payment account associated with the payment certificate base is opened in the step of performing the payment operation.

76. The method according to claim 74, *characterized* in that the crediting operation is carried out in the step of performing the payment operation.

77. The method according to claim 74, *characterized* in that in the step of performing the payment operation the signed payer order is entered into the operator's information storage.

78. The method according to claim 74, *characterized* in that in the step of replenishing the payer device a money demand is formed including data for making a blind money signature, and is delivered to the payment server in which a replenishment source and replenishment amount are determined according to the money demand; data to be unblinded are created in the step of making the blind money signature by processing data for making the blind money signature, that are comprised in the demand, with a secret money key corresponding to the replenishment amount, whereupon the payment certificate signature is made in the payer device by unblinding.

79. The method according to claim 78, *characterized* in that in the step of replenishing the payer device by the operation of primarily filling the payment certificate a blinded identi-

fier of the created payment certificate base is included as the data for making the blind money signature into the money demand being formed.

80. The method according to claim 78, *characterized* in that in the step of replenishing the payer device by the operation of replenishing the payment certificate a blinded payment certificate signature is included as the data for making the blind money signature into the money demand being formed.

81. The method according to claim 74, *characterized* in that in the step of performing the payment operation a payee receipt is included into the operator's response to the payee order, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payee is judged according to the validity of the signature on the payee receipt.

82. The method according to claim 74, *characterized* in that in the step of performing the payment operation data are formed in the payee device with the use of the operator's response to the payee order and delivered to the payer device, according to which data the performing of the payment for the payer is judged.

83. The method according to claim 82, *characterized* in that in the step of performing the payment operation a payer receipt is included into the operator's response to the payee order and into the data delivered to the payer device, which receipt being signed with the arbitrary secret key of the operator, and the performing of the payment for the payer is judged according to the validity of the signature on the payer receipt.

84. The method according to claim 83, *characterized* in that the payer receipt is encrypted by an arbitrary encryption key of the payer prior to including said receipt into the operator's response to the payee order.

85. The method according to claim 74, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate converted by an arbitrary one-way function is used as the identifier of the payment certificate base.

86. The method according to claim 74, *characterized* in that in performing operations with the payment certificate the public key of the payment certificate is used as the identifier of the public key of the payment certificate.

87. The method according to claim 74, *characterized* in that in the step of replenishing the payer device the validity of the made payment certificate signature is verified.

88. The method according to claim 74, *characterized* in that in the step of opening the account an arbitrary secret key is accepted as the secret key of the account, and the public key corresponding to the secret key of the account is delivered to the payment server as a public key of the account being opened.

89. The method according to claim 74, *characterized* in that conditions of payment are included into the payer order.

90. The method according to claim 89, *characterized* in that payee obligation data are included into the conditions of payment comprised in the payer order.

91. The method according to claim 90, *characterized* in that prior to performing the payment operation, the payee obligation data are signed with an arbitrary secret key of the payee, and the payer verifies the payee's signature on the payee obligation data prior to performing the payment operation.

92. The method according to claim 89, *characterized* in that in the payer device in the step

of forming the payment data, the payee obligation data are processed by an arbitrary one-way function, and data obtained in this processing are included into the payer order as the conditions of payment.

93. The method according to claim 74, *characterized* in that the payer order is encrypted by an arbitrary public encryption key of the operator prior to including them into the payment data.

94. The method according to claim 74, *characterized* in that in the step of replenishing the payer device a payer's account is used as a replenishment source.

95.. The method according to claim 74, *characterized* in that in the step of replenishing the payer device a bank card is used as a replenishment source.

96. The method according to claim 74, *characterized* in that in the step of performing the payment operation the payee appears as the payer.

97. The method according to claim 74, *characterized* in that in the step of performing the payment operation a part of a payment certificate value is returned to the payer device.

98. The method according to claim 74, *characterized* in that in the step of replenishing the payer device, a payment account associated with the base of one of payment certificates is used as a replenishment source.

99. The method according to claim 74, *characterized* in that the step of replenishing the payer device is performed from funds of an intermediate payer.

100. The method according to claim 99, *characterized* in that in the step of replenishing the payer device, data blinded in the payer device in the step of making the blind money signature of the operator are subjected to an additional blinding in the payer device of the intermediate payer.

101. An apparatus for effecting payments comprising a payer device, payee device and payment server interconnected by telecommunication nets, the payer device comprising a means for replenishing the payer device by the use of making a blind money signature of an operator, and the payment server comprising a means for making a money signature, *characterized* in that the payer device further comprises a means for creating a payment certificate base by processing a public key of the payment certificate with a one-way function, a means for storing the created payment certificate base in a storage device, and a means for forming a payer order signed with a secret key of the payment certificate; the payee device comprises a means for forming a payee order including the payer order; the payment server further comprises a means for performing a payment operation, a means for serving a database of payment accounts, and a means for serving a database of accounts, wherein said means for performing a payment operation has a means for verifying a signature on the payer order and a means for making a signed payee receipt, said means for serving the database of payment accounts has a means for verifying the money signature, and the means for replenishing the payer device by the use of making the blind money signature of the operator is realized using a means for increasing the level of the payment certificate signature.

102. The apparatus according to claim 101, *characterized* in that the payee device comprises a means for opening a public key account, and said means for serving the database of accounts has a means for opening a public key account.

103. The apparatus according to claim 101, *characterized* in that the payer device comprises a means for opening a public key account, and said means for serving the database of accounts has a means for opening a public key account.

104. The apparatus according to claim 101, *characterized* in that said means for increasing the level of the payment certificate signature has a means for forming a money demand including a blinded payment certificate signature, a means for unblinding the data to be unblinded comprised in a response to the money demand, and a means for entering the result of unblinding into said storage device, and the payment server comprises a means for processing the money demand, wherein said means for processing the money demand has a means for making the money signature.

105. The apparatus according to claim 101, *characterized* in that said means for serving the database of payment accounts has a means for opening a payment account and a means for crediting a payment account.

106. The apparatus according to claim 101, *characterized* in that the payee device has a means for verifying the signed payee receipt.

107. The apparatus according to claim 101, *characterized* in that said means for forming the payer order signed with the secret key of the payment certificate has a means for forming a demand for crediting the payment account.

108. The apparatus according to claim 101, *characterized* in that said means for forming the demand for crediting the payment account has a means for decreasing the level of the payment certificate signature.

109. The apparatus according to claim 101, *characterized* in that the payer device, payee device and payment server are further provided with a means for encryption of outgoing messages and a means for decryption of incoming messages.